

Office of the Secretary of Defense

§ 311.3

of either the reports required by paragraph (p) of the Privacy Act, or Section 3514 of Pub. L. 96-511.

8. *Use of Contractors.* Matching programs should, as far as practicable, be conducted “in-house” by federal agencies using agency personnel, rather than by contract. When contractors are used, however,

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor’s performance of the matching program. The contract should include the Privacy Act clause required by Federal Personnel Regulation Amendment 155 (41 CFR 1-1.337-5);

b. The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, GSA, and the Department of Commerce;

c. The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor’s own use;

d. Contractor personnel involved in the matching program shall be made explicitly aware of their obligations under the Act and of these guidelines, agency rules, and any special safeguards in relation to each specific match performed.

e. Any disclosures of records by the agency to the contractor should be made pursuant to a “routine use” (5 U.S.C. 552a(b)(3)).

F. *Implementation and Oversight.* OMB will oversee the implementation of these guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

PART 311—OSD PRIVACY PROGRAM

Sec.

311.1 Purpose.

311.2 Applicability and scope.

311.3 Definitions.

311.4 Policy.

311.5 Responsibilities.

311.6 Procedures.

311.7 Information requirements.

311.8 Procedures for exemptions.

AUTHORITY: Pub. L. 93-579, 88 Stat. 1986 (5 U.S.C. 552a).

SOURCE: 64 FR 22785, Apr. 28, 1999, unless otherwise noted.

§ 311.1 Purpose.

This part updates and implements basic policies and procedures outlined in 5 U.S.C. 552a, OMB Circular A-130,¹ and DoD 5400.11-R² and provides guidance and procedures for use in establishing the Privacy Program in the Office of the Secretary of Defense (OSD) and those organizations assigned to OSD for administrative support.

§ 311.2 Applicability and scope.

This part:

(a) Applies to the OSD, the Chairman of the Joint Chiefs of Staff, Uniformed Services University of the Health Sciences (USUHS) and other activities assigned to OSD for administrative support hereafter referred to collectively as “OSD Components.”

(b) Covers record systems maintained by OSD Components and governs the maintenance, access, change, and release of information contained in OSD Component record systems, from which information about an individual is retrieved by a personal identifier.

§ 311.3 Definitions.

Access. Any individual’s review of a record or a copy of a record or parts of a system of records.

Disclosure. The transfer of any personal information from a system of records by any means of oral, written, electronic, mechanical, or other communication, to any person, private entity, or Government agency, other than the subject of the record, the subject’s designated agent, or the subject’s guardian.

Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf.

Individual access. Access to personal information pertaining to the individual, by the individual, his or her designated agent or legal guardian.

¹Copies may be obtained by contacting EOP Publications, 725 16th Street, NW., NEOB, Washington, DC 20503.

²Copies may be obtained via internet at <http://web7.whs.osd.mil/corres.htm>.

§ 311.4

32 CFR Ch. I (7–1–02 Edition)

Maintain. Includes maintenance, collection, use or dissemination.

Personal information. Information about an individual that is intimate or private, as distinguished from information related solely to the individual's official functions or public life.

§ 311.4 Policy.

(a) It is DoD policy to safeguard personal information contained in any system of records maintained by any DoD Component and to permit any individual to know what existing records pertain to him or her in any OSD Component covered by this part.

(b) Each office maintaining records and information about individuals shall ensure that their privacy is protected from unauthorized disclosure of personal information. These offices shall permit individuals to have access to, and to have a copy made of all, or any portion of records about them, except as provided in Chapters 3 and 5, DoD 5400.11–R, and to have an opportunity to request that such records be amended as provided by the Privacy Act of 1974 and Chapter 3 of DoD 5400.11–R. Individuals requesting access to their records shall receive concurrent consideration under 5 U.S.C. 552a and the Freedom of Information Act, as amended, if appropriate.

(c) Heads of OSD Components shall maintain any necessary record of a personal nature that is individually identifiable in a manner that complies with the law and DoD policy. Any information collected must be as accurate, relevant, timely, and complete as is reasonable to ensure fairness to the individual. Adequate safeguards must be provided to prevent misuse or unauthorized release of such information.

§ 311.5 Responsibilities.

(a) The Director of Administration and Management, Office of the Secretary of Defense (DA&M, OSD) shall:

(1) Direct and administer the DoD Privacy Program for OSD Components.

(2) Establish standards and procedures to ensure implementation of and compliance with the Privacy Act of 1974, OMB Circular No. A–130, and DoD 5400.11–R.

(3) Designate the Director for Freedom of Information and Security Re-

view as the point of contact for individuals requesting information of access to records and copies about themselves.

(4) Serve as the appellate authority within OSD when a requester appeals a denial for access to records under the Privacy Act.

(5) Serve as the appellate authority within OSD when a requester appeals a denial for amendment of a record or initiates legal action to correct a record.

(6) Evaluate and decide, in coordination with The General Counsel of the Department of Defense (GC, DoD), appeals resulting from denials of access or amendments to records by the OSD Components.

(7) Designate the Directives and Records Division, Correspondence and Directives Directorate, Washington Headquarters Services (WHS) as the office responsible for all aspects of the Privacy Act, except that portion about receiving and acting on public requests for personal records. As such, the Directives and Records Division shall:

(i) Exercise oversight and administrative control of the Privacy Act Program in OSD and those organizations assigned to OSD for administrative support.

(ii) Provide guidance and training to organizational entities as required by 5 U.S.C. 552a and OMB Circular A–130. Periodic training will be provided to public affairs officers and others who may be expected to deal with the news media or the public.

(iii) Collect and consolidate data from OSD Components, and submit an annual report to the Defense Privacy Office, as required by 5 U.S.C. 552a, OMB Circular A–130, and DoD 5400.11–R.

(iv) Coordinate and consolidate information for reporting all record systems, as well as changes to approved systems, to the OMB, the Congress, and the FEDERAL REGISTER, as required by 5 U.S.C. 552a, OMB Circular E A–130, and DoD 5400.11–R.

(v) Collect information from OSD Components, and prepare consolidated reports required by 5 U.S.C. 552a and DoD 5400.11–R.

(b) The Director for Freedom of Information and Security Review shall:

(1) Forward requests for information or access to records to the appropriate

OSD Component having primary responsibility for any pertinent system of records under 5 U.S.C. 552a, or to OSD Components, under the Freedom of Information Act, as amended.

(2) Maintain deadlines to ensure that responses are made within the time limits prescribed in DoD 5400.7-R,³ DoD Instruction 5400.10,⁴ and this part.

(3) Collect fees charged and assessed for reproducing requested materials.

(4) Refer all matters about amendments of records and general and specific exemptions under the 5 U.S.C. 552a to the proper OSD Components.

(c) The General Counsel of the Department of Defense shall:

(1) Coordinate all OSD final denials of appeals for amending records, and review actions to confirm denial of access to records, as appropriate.

(2) Provide advice and assistance to the DA&M, OSD in the discharge of appellate and review responsibilities, and to the DFOISR on all access matters.

(3) Provide advice and assistance to OSD Components on legal matters pertaining to the Privacy Act of 1974.

(d) The Heads of the OSD Components shall:

(1) Designate an individual as the point of contact for Privacy Act matters; designate an official to deny initial requests for access to an individual's records or changes to records; and advise both DA&M, OSD and DFOISR of names of officials so designated.

(2) Report any new record system, or changes to an existing system, to the Chief, Directives and Records Division, WHS, at least 90 days before the intended use of the system.

(3) Review all contracts that provide for maintaining records systems, by or on behalf of his or her office, to ensure within his or her authority, that language is included that provides that such systems shall be maintained in a manner consistent with 5 U.S.C. 552a.

(4) Revise procurement guidance to ensure that any contract providing for the maintenance of a records system, by or on behalf of his or her office, includes language that ensures that such system shall be maintained in accordance with 5 U.S.C. 552a.

(5) Revise computer and telecommunications procurement policies to ensure that agencies review all proposed contracts for equipment and services to comply with 5 U.S.C. 552a.

(6) Coordinate with Automatic Data Processing (ADP) and word processing managers providing services to ensure that an adequate risk analysis is conducted to comply with DoD 5400.11-R.

(7) Review all Directives that require forms or other methods used to collect information about individuals to ensure that they are in compliance with 5 U.S.C. 552a.

(8) Establish administrative systems in OSD Component organizations to comply with the procedures listed in this part and DoD 5400.11-R.

(9) Coordinate with the GC, DoD on all proposed denials of access to records.

(10) Provide justification to the DFOISR when access to a record is denied in whole or in part.

(11) Provide the record to the DFOISR when the initial denial of a request for access to such record has been appealed by the requester, or at the time of initial denial when appeal seems likely.

(12) Maintain an accurate account of the actions resulting in a denial for access to a record or for the correction of a record. This account should be maintained so that it can be readily certified as the complete record of proceedings if litigation occurs.

(13) Ensure that all personnel who either have access to the system of records, or who are engaged in developing or supervising procedures for handling records in the system, are aware of their responsibilities for protecting personal information as established in the Privacy Act and DoD 5400.11-R.

(14) Forward all requests for access to records received directly from an individual to the DFOISR for appropriate suspense control and recording.

(15) Provide DFOISR with a copy of the requested record when the request is granted.

(e) The requester who desires to submit a request is responsible for:

(1) Determining whether to submit the request in writing or in person. A requester who seeks access to records

³See footnote 2 to § 311.1.

⁴See footnote 2 to § 311.1.

§311.6

32 CFR Ch. I (7–1–02 Edition)

pertaining to himself or herself which are filed by his or her name or personal identifier:

(i) May make such a request in person to the custodian of the records. If the requester is not satisfied with the response, however, in order to invoke any provision of 5 U.S.C. 552a, DoD 5400.11–R, or this part, the requester must file a request in writing as provided in §311.6(b)(10). The requester must provide proof of identity by showing drivers license or similar credentials.

(ii) Describing the record sought, and providing sufficient information to enable the material to be located (e.g., identification of system of records, approximate date it was initiated, originating organization, and type of document).

(iii) Complying with procedures provided in DoD 5400.11–R for inspecting and/or obtaining copies of requested records.

(iv) Submitting a written request to amend the record to the system manager or to the office designated in the system notice.

[64 FR 22785, Apr. 28, 1999, as amended at 66 FR 41780, Aug. 9, 2001]

§311.6 Procedures.

(a) *Publication of notice in the Federal Register.* (1) A notice shall be published in the FEDERAL REGISTER of any record system meeting the definition of a system of records in DoD 5400.11–R.

(2) Regarding new or revised records systems, each OSD Component shall provide the Chief, Directives and Records Division with 90 days advance notice of any anticipated new or revised system of records. This material shall be submitted to the OMB and to Congress at least 60 days before use and to the Federal Register at least 30 days before being put into use, to provide an opportunity for interested persons to submit written data, views, or arguments to the OSD Components. Instructions on content and preparation are outlined in DoD 5400.11–R.

(b) *Access to information on records systems.* (1) Upon request, and as provided by the Privacy Act, records shall be disclosed only to the individual they pertain to and under whose individual name or identifier they are filed, un-

less exempted by provisions stated in DoD 5400.11–R.

(2) There is not requirement under 5 U.S.C. 552a that a record be created or that an individual be given access to records that are not in a group of records that meet this definition of a system of records in 5 U.S.C. 552a.

(3) Granting access to a record containing personal information shall not be conditioned upon any requirement that the individual state a reason or otherwise justify the need to gain access.

(4) No verification of identity shall be required of an individual seeking access to records that are otherwise available to the public.

(5) Individuals shall not be denied access to a record in a system of records about themselves because those records are exempted from disclosure under DoD 5400.7–R. Individuals may only be denied access to a record in a system of records about themselves when those records are exempted from the access provisions of the Privacy Act under DoD 5400.11–R, Chapter 5.

(6) Individuals shall not be denied access to their records for refusing to disclose their Social Security Numbers (SSNs), unless disclosure of the SSN is required by statute, by regulation adopted before January 1, 1975, or if the record's filing identifier and only means of retrieval is by SSN.

(7) Individuals may request access to their records, in person or by mail, in accordance with the procedures outlined in paragraph (b)(8) of this section.

(8) Information necessary to identify a record is: the individual's name, date of birth, place of birth, identification of the records system as listed in the FEDERAL REGISTER, or sufficient information to identify the type of records being sought, and the approximate date the records might have been created. Any individual making a request for access to records in person shall come to the Directorate for Freedom of Information and Security Review (DFOISR), Room 2C757, Pentagon, Washington, DC 20301–1155; and shall provide personal identification acceptable to the Director, DFOISR, to verify the individual's identity (e.g., driver's license, other licenses, permits, or

passes used for routine identification purposes).

(9) If an individual wishes to be accompanied by a third party when seeking access to records or wishes to have the record released directly to a third party, the individual may be required to furnish a signed access authorization granting the third party access.

(10) Any individual submitting a request by mail for access to information shall address such request to the Directorate for Freedom of Information and Security Review, Pentagon, Room 2C757, Washington, DC 20301-1155. To verify the identity of the individual, the request shall include either a signed notarized statement or an unsworn declaration in the format specified by 28 U.S.C. 1746.

(11) The following procedures shall apply to requests for access to records or information compiled for law enforcement purposes:

(i) Individuals requesting access to records or information about themselves and compiled for law enforcement purposes are processed under DoD 5400.11-R and DoD 5400.7-R to give them the greater degree of access.

(ii) Individual requests for access to records or information about themselves and compiled for law enforcement purposes (and in the custody of law enforcement activities) that have been incorporated into the records system, exempted from the access provisions of 5 U.S.C. 552a, will be processed in accordance with subsection C1.5.13 and Chapter 5, DoD 5400.7-R. Individuals shall not be denied access to records solely because they are in the exempt system, but they will have the same access that they would receive under DoD 5400.7-R. (Also see subsection A.10., Chapter 3, DoD 5400.11-R.)

(iii) Requests by the individuals for access to records or information about themselves and compiled for law enforcement purposes that are in records systems exempted from access provisions will be processed under subsection C.1., Chapter 5 of DoD 5400.11-R or DoD 5400.7-R, depending upon which regulation gives the greater degree of access. (See also subsection A. 10., Chapter 3, DoD 5400.1-R)

(iv) Individual requests for access to records or information about themselves and compiled for law enforcement purposes exempted from access under Section B, Chapter 5 of DoD 54.11-R, that are temporarily in the hands of a non-law enforcement element for adjudicative or personnel actions, shall be referred to the originating agency. The requester will be informed in writing of these referrals.

(12) The following procedures shall apply to requests for illegible, incomplete, or partially exempt records:

(i) An individual shall not be denied access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available (e.g., deteriorated state or on magnetic tape). The document will be prepared as an extract, or it will be exactly recopied.

(ii) If a portion of the record contains information that is exempt from access, an extract or summary containing all of the information in the record that is releasable shall be prepared.

(iii) When the physical condition to the record makes it necessary to prepare an extract for release, the extract shall be prepared so that the requester will understand it.

(iv) The requester shall be informed of all deletions or changes to records.

(13) Medical records shall be disclosed to the individual they pertain to, unless a determination is made in consultation with a medical doctor, that the disclosure could have adverse effects on the individual's physical or mental health. Such information may be transmitted to a medical doctor named by the individual concerned. If the named medical doctor declines to provide the record to the individual, the OSD Components shall take positive action to ensure that the requested records are provided the individual.

(14) The individual may be charged reproduction fees for copies or records as outlined in DoD 5400.11-R.

(c) *Requested to amend personal information in records systems and disputes.*

(1) The Head of an OSD Component, or the designated official, shall allow individuals to request amendment to their records to the extent that such

records are not accurate, relevant, timely, or complete. Requests should be as brief and as simple as possible and should contain, as a minimum, identifying information to locate the record, as description of the items to be amended, and the reason for a change. A request shall not be rejected nor required to be resubmitted unless additional information is essential to process the request. Requesters shall be required to provide verification of their identity as stated in paragraph (b)(8) of this section, to ensure that they are seeking to amend records about themselves, and not, inadvertently or intentionally, the records of others.

(2) The appropriate system manager shall mail a written acknowledgement to an individual's request to amend a record within 10 days after receipt, excluding Saturdays, Sundays, and legal public holidays. Such acknowledgement shall identify the request and may, if necessary, request any additional information needed to make a determination. No acknowledgment is necessary if the request can be reviewed, processed, and if the individual can be notified of compliance or denial within the 10-day period. Whenever practical, the decision shall be made within 30 working days. For requests presented in person, written acknowledgment may be provided at the time the request is presented.

(3) The Head of an OSD Component, or designated official, shall promptly take one of the following actions on requests to amend the records:

(i) If the OSD Component official agrees with any portion or all of an individual's request, he or she will proceed to amend the records in accordance with existing statutes, regulations, or administrative procedures, and inform the requester of the action taken. The OSD Component official shall also notify all previous holders of the record that the amendment has been made, and shall explain the substance of the correction.

(ii) If the OSD Component official disagrees with all or any portion of a request, the individual shall be informed promptly of the refusal to amend a record, the reason for the refusal, and the procedure established by

OSD for an appeal as outlined in paragraph (c)(6) of this section.

(iii) If the request for an amendment pertains to a record controlled and maintained by another Federal Agency, the request shall be referred to the appropriate Agency, and the requester advised of this:

(4) The following procedures shall be used when reviewing records under dispute:

(i) In response to a request for an amendment to records, officials shall determine whether the requester has adequately supported their claim that the record is inaccurate, irrelevant, untimely, or incomplete.

(ii) The Head of an OSD Component, or designated official, shall limit the review of a record of those items of information that clearly bear on any determination to amend the records and shall ensure that all those elements are present before determination is made.

(5) If the Head of an OSD Component, or designated official, after an initial review of a request to amend a record, disagrees with all or any portion of a record, he or she shall:

(i) Advise the individual of the denial and the reason for it.

(ii) Inform the individual that he or she may appeal the denial.

(iii) Describe the procedures for appealing the denial including the name and address of the official to whom the appeal should be directed. The procedures should be as brief and simple as possible.

(iv) Furnish a copy of the justification of any denial to amend a record to the DA&M, OSD.

(6) If an individual disagrees with the initial OSD determination, he or she may file an appeal. The request should be sent to the Director of Administration and Management, Office of the Secretary of Defense (DA&M, OSD), 1950 Defense Pentagon, Washington, D.C. 20301-1950, if the record is created and maintained by an OSD Component.

(7) If, after review, the DA&M, OSD further refuses to amend the record as requested, he shall advise the individual:

(i) Of the refusal and the reason and authority for the denial.

(ii) Of his or her right to file a statement of the reason for disagreeing with the DA&M's decision.

(iii) Of the procedures for filing a statement of disagreements.

(iv) That the statement filed shall be made available to anyone the record is disclosed to, together with a brief statement, at the discretion of the OSD Component, summarizing its reasons for refusing to amend the records.

(v) That prior recipients of copies of disputed records be provided by a copy of any statement of dispute to the extent that an accounting of disclosure is maintained.

(vi) Of his or her right to seek judicial review of the DA&M's refusal to amend a record.

(8) If, after the review, the DA&M, OSD, determines that the record should be amended in accordance with the individual's request, the OSD Component shall amend the record, advise the individual, and inform previous recipients where an accounting of disclosure has been maintained.

(9) All appeals should be processed within 30 days (excluding Saturdays, Sundays, and legal public holidays) after receipt by the proper office. If the DA&M determines that a fair and equitable review cannot be made within that time, the individual shall be informed in writing of the reasons for the delay and of the approximate date the review is expected to be completed.

(d) Disclosure of disputed information.

(1) If the DA&M, OSD, has refused to amend a record and the individual has filed a statement under paragraph (c)(7) of this section, the OSD Component shall clearly annotate the disputed record so that it is apparent to any person to whom the record is disclosed that a statement has been filed. Where feasible, the notation itself shall be integral to the record. Where an accounting of a disclosure has been made, the OSD Component shall advise previous recipients that the record has been disputed and shall provide a copy of the individual's statement.

(i) This statement shall be maintained to permit ready retrieval whenever the disputed portion of the record is to be disclosed.

(ii) When information that is the subject of a statement of dispute is subse-

quently disclosed, the OSD Component's designated official shall note which information is disputed and provide a copy of the individual's statement.

(2) The OSD Component shall include a brief summary of its reasons for not making a correction when disclosing disputed information. Such statement shall normally be limited to the reasons given to the individual for not amending the record.

(3) Copies of the OSD Component's summary will be treated as part of the individual's record; however, it will not be subject to the amendment procedure outlined in paragraph (c)(3)(iii) of this section.

(e) Penalties—(1) Civil action. (i) An individual may file a civil suit against the United States and may recover damages, for:

(A) Refusal to amend a record.

(B) Improper denial of the access to a record.

(C) Failure to maintain an accurate, relevant, timely, and complete record that is used to make determinations adverse to the individual.

(ii) An individual may also file a suit against the United States for failure to implement a provision of the Privacy Act when such failure leads to an adverse determination.

(iii) If the individual's suit is upheld, the court may direct the United States to pay the court costs and attorney's fees.

(2) Criminal action. (i) Criminal penalties may be imposed against an OSD officer or employee for certain offenses listed in section (i) of the Privacy Act, as follows: willful unauthorized disclosure of protected information in the records; failure to publish a notice of the existence of a record system in the FEDERAL REGISTER; requesting or gaining access to the individual's record under false pretenses.

(ii) An OSD officer or employee may be fined up to \$5,000 for a violation as outlined in paragraph (e)(2)(i) of this section.

(3) Litigation status sheet. Whenever a complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the Department of Defense, a DoD component, or any DoD employee, the responsible system manager shall promptly

notify the Defense Privacy Office. The litigation status sheet in DoD 5400.II-R provides a standard format for this notification. (The initial litigation status sheet shall, as a minimum, provide the information required by items 1. through 6.) A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment or opinion shall be provided to the Defense Privacy Office with the litigation status sheet reporting that judgment or opinion.

(f) *Computer matching programs.* Paragraph B of Chapter 11 of DoD 5400.11-R prescribes that all requests for participation in a matching program (either as a matching agency or a source agency) be submitted to the Defense Privacy Office for review and compliance. OSD Components shall submit these request through the Directives and Records Division.

[64 FR 22785, Apr. 28, 1999; 64 FR 27694, May 21, 1999]

§311.7 Information requirements.

The Defense Privacy Office shall establish requirements and deadlines for DoD privacy reports. These reports shall be licensed in accordance with DoD Directive 8910.1.⁵

§311.8 Procedures for exemptions.

(a) *General information.* The Secretary of Defense designates those Office of the Secretary of Defense (OSD) systems of records which will be exempt from certain provisions of the Privacy Act. There are two types of exemptions, general and specific. The general exemption authorizes the exemption of a system of records from all but a few requirements of the Act. The specific exemption authorizes exemption of a system of records or portion thereof, from only a few specific requirements. If an OSD Component originates a new system of records for which it proposes an exemption, or if it proposes an additional or new exemption for an existing system of records, it shall submit the recommended exemption with the records system notice as outlined in §311.6. No exemption of a system of records shall be considered automatic

for all records in the system. The systems manager shall review each requested record and apply the exemptions only when this will serve significant and legitimate Government purpose.

(b) *General exemptions.* The general exemption provided by 5 U.S.C. 552a(j)(2) may be invoked for protection of systems of records maintained by law enforcement activities. Certain functional records of such activities are not subject to access provisions of the Privacy Act of 1974. Records identifying criminal offenders and alleged offenders consisting of identifying data and notations of arrests, the type and disposition of criminal charges, sentencing, confinement, release, parole, and probation status of individuals are protected from disclosure. Other records and reports compiled during criminal investigations, as well as any other records developed at any stage of the criminal law enforcement process from arrest to indictment through the final release from parole supervision are excluded from release.

(1) *System identifier and name:* DWHS P42.0, DPS Incident Reporting and Investigations Case Files.

(i) *Exemption.* Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, Sections (c) (3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5); and (h) of the Act.

(ii) *Authority:* 5 U.S.C. 552a(j)(2).

(iii) *Reason:* The Defense Protective Service is the law enforcement body for the jurisdiction of the Pentagon and immediate environs. The nature of certain records created and maintained by the DPS requires exemption from access provisions of the Privacy Act of 1974. The general exemption, 5 U.S.C. 552a(j)(2), is invoked to protect ongoing investigations and to protect from access criminal investigation information contained in this record system, so as not to jeopardize any subsequent judicial or administrative process taken as a result of information contained in the file.

(2) *System identifier and name:* JS006.CND, Department of Defense Counternarcotics C4I System.

⁵ See footnote 2 to §311.1.

(i) Exemption: Portions of this system that fall within 5 U.S.C. 552a(j)(2) are exempt from the following provisions of 5 U.S.C. 552a, section (c) (3) and (4); (d)(1) through (d)(5); (e)(1) through (e)(3); (e)(4)(G) and (e)(4)(H); (e)(5); (f)(1) through (f)(5); (g)(1) through (g)(5) of the Act.

(ii) Authority: 5 U.S.C. 552a(j)(2).

(iii) Reason: From subsection (c)(3) because the release of accounting of disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede USSOUTHCOM's criminal law enforcement.

(iv) For subsections (c)(4) and (d) because notification would alert a subject to the fact that an investigation of that individual is taking place, and might weaken the on-going investigation, reveal investigatory techniques, and place confidential informants in jeopardy.

(v) From subsections (e)(4) (G) and (H) because this system of records is exempt from the access provisions of subsection (d) pursuant to subsection (j).

(vi) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going criminal investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(vii) For compatibility with the exemption claimed from subsection (f), the civil remedies provisions of subsection (g) must be suspended for this record system. Because of the nature of criminal investigations, standards of accuracy, relevance, timeliness and

completeness cannot apply to this record system. Information gathered in criminal investigations is often fragmentary and leads relating to an individual in the context of one investigation may instead pertain to a second investigation.

(viii) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to USSOUTHCOM's close liaison and working relationships with the other Federal, as well as state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(ix) From subsection (e)(2) because collecting information to the greatest extent possible directly from the subject individual may or may not be practicable in a criminal investigation. The individual may choose not to provide information and the law enforcement process will rely upon significant information about the subject from witnesses and informants.

(x) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal investigation. The effect would be somewhat inimical to established investigative methods and techniques.

(xi) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the criminal investigative process. It is the nature of criminal law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significant as

further investigation brings new details to light.

(xii) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(c) *Specific exemptions.* All systems of records maintained by any OSD Component shall be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to subsection (k)(1) of that section to the extent that the system contains any information properly classified under Executive Order 11265, 'National Security Information,' dated June 28, 1979, as amended, and required by the Executive Order to be kept classified in the interest of national defense or foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions may contain isolated information which has been properly classified. The Secretary of Defense has designated the following OSD system of records described below specifically exempted from the appropriate provisions of the Privacy Act pursuant to the designated authority contained therein:

(1) *System identifier and name:* DGC 16, Political Appointment Vetting Files.

(i) *Exemption.* Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might

refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source.

(2) *System identifier and name:* DWHS P28, The Office of the Secretary of Defense Clearance File.

(i) *Exemption.* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information but only to the extent that disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning the specific information which would reveal the identity of the source.

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This exemption is required to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(3) *System identifier and name:* DGC 04, Industrial Personnel Security Clearance Case Files.

(i) *Exemption.* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of Title 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* This system of records is exempt from subsections (c)(3) and (d) of section 552a of 5 U.S.C. which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence, or prior to September 27, 1975, under an implied

promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(4) *System identifier and name:* DWHS P32, Standards of Conduct Inquiry File.

(i) *Exemption.* This system of records is exempted from subsections (c)(3) and (d) of 5 U.S.C. 552a, which would require the disclosure of: Investigatory material compiled for law enforcement purposes; or investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, or Federal contracts, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. If any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or otherwise be eligible, as a result of the maintenance of investigatory material compiled for law enforcement purposes, the material shall be provided to that individual, except to the extent that its disclosure would reveal the identity of a source who furnished information to the Government under an express promise or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(ii) *Authority.* 5 U.S.C. 552a(k) (2) and (5).

(iii) *Reasons.* These exemptions are necessary to protect the confidentiality of the records compiled for the

purpose of: enforcement of the conflict of interest statutes by the Department of Defense Standards of Conduct Counselor, General Counsel, or their designees; and determining suitability, eligibility or qualifications for Federal civilian employment, military service, or Federal contracts of those alleged to have violated or caused others to violate the Standards of Conduct regulations of the Department of Defense.

(5) *System identifier and name:* DUSDP 02, Special Personnel Security Cases.

(i) *Exemption:* All portions of this system which fall under 5 U.S.C. 552a(k)(5) are exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority:* 5 U.S.C. 552a(k)(5).

(iii) *Reasons:* This system of records is exempt from subsections (c)(3) and (d) of 5 U.S.C. 552a which would require the disclosure of investigatory material compiled solely for the purpose of determining access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an expressed promise that the identity of the source would be held in confidence or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. A determination will be made at the time of the request for a record concerning whether specific information would reveal the identity of a source. This exemption is required in order to protect the confidentiality of the sources of information compiled for the purpose of determining access to classified information. This confidentiality helps maintain the Government's continued access to information from persons who would otherwise refuse to give it.

(6) *System identifier and name:* DODDS 02.0, Educator Application Files.

(i) *Exemption.* All portions of this system which fall within 5 U.S.C. 552a(k)(5) may be exempt from the following provisions of 5 U.S.C. 552a: (c)(3); (d).

(ii) *Authority.* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* It is imperative that the confidential nature of evaluation and investigatory material on teacher application files furnished the Department of Defense Dependent Schools

(DoDDS) under promises of confidentiality be exempt from disclosure to the individual to insure the candid presentation of information necessary to make determinations involving applicants suitability for DoDDS teaching positions.

(7) *System identifier and name:* DGC 20, DoD Presidential Appointee Vetting File.

(i) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Portions of this system of records that may be exempt pursuant to 5 U.S.C. 552a(k)(5) are subsections (d)(1) through (d)(5).

(ii) *Authority:* 5 U.S.C. 552a(k)(5).

(iii) *Reason:* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(8) *System identifier and name:* DWHS P29, Personnel Security Adjudications File.

(i) *Exemption:* Portions of this system of records that fall within the provisions of 5 U.S.C. 552a(k)(5) may be exempt from the following subsections (d)(1) through (d)(5).

(ii) *Authority:* 5 U.S.C. 552a(k)(5).

(iii) *Reasons.* From (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might

refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(9) *System identifier and name:* JS004SECDIV, Joint Staff Security Clearance Files.

(i) *Exemption:* Portions of this system of records are exempt pursuant to the provisions of 5 U.S.C. 552a(k)(5) from subsections 5 U.S.C. 552a(d)(1) through (d)(5).

(ii) *Authority:* 5 U.S.C. 552a(k)(5).

(iii) *Reasons:* From subsections (d)(1) through (d)(5) because the agency is required to protect the confidentiality of sources who furnished information to the government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it. This exemption is limited to disclosures that would reveal the identity of a confidential source. At the time of the request for a record, a determination will be made concerning whether a right, privilege, or benefit is denied or specific information would reveal the identity of a source.

(10) *System identifier and name:* DFMP 26, Vietnamese Commando Compensation Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(ii) *Authority:* 5 U.S.C. 552a(k)(1).

(iii) *Reasons:* From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1–R, may cause damage to the national security.

(11) *System identifier and name:* DUSP 11, POW/Missing Personnel Office Files.

(i) *Exemption:* Information classified under E.O. 12958, as implemented by DoD 5200.1–R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

Office of the Secretary of Defense

§ 312.6

(ii) *Authority*: 5 U.S.C. 552a(k)(1).

(iii) *Reasons*: From subsection 5 U.S.C. 552a(d) because granting access to information that is properly classified pursuant to E.O. 12958, as implemented by DoD 5200.1-R, may cause damage to the national security.

[65 FR 53168, Sept. 1, 2000, as amended at 66 FR 41780, Aug. 8, 2001]

PART 312—OFFICE OF THE INSPECTOR GENERAL (OIG) PRIVACY PROGRAM

Sec.

312.1 Purpose.

312.2 Definitions.

312.3 Procedure for requesting information.

312.4 Requirements for identification.

312.5 Access by subject individuals.

312.6 Fees.

312.7 Request for correction or amendment.

312.8 OIG review of request for amendment.

312.9 Appeal of initial amendment decision.

312.10 Disclosure of OIG records to other than subject.

312.11 Penalties.

312.12 Exemptions.

312.13 Ownership of OIG investigative records.

312.14 Referral of records.

AUTHORITY: Pub. L. 93-579, 88 Stat 1896 (5 U.S.C. 552a).

SOURCE: 56 FR 51976, Oct. 17, 1991, unless otherwise noted.

§ 312.1 Purpose.

Pursuant to the requirements of the Privacy Act of 1974 (5 U.S.C. 552a) and 32 CFR part 286a-DoD Privacy Program, the following rules of procedures are established with respect to access and amendment of records maintained by the Office of the Inspector General (OIG) on individual subjects of these records.

§ 312.2 Definitions.

(a) All terms used in this part which are defined in 5 U.S.C. 552a shall have the same meaning herein.

(b) As used in this part, the term "agency" means the Office of the Inspector General (OIG), Department of Defense.

§ 312.3 Procedure for requesting information.

Individuals should submit inquiries regarding all OIG files by mail to the

Assistant Inspector General for Investigations, ATTN: FOIA/PA Division, 400 Army Navy Drive, Arlington, VA 22202-2884. All personal visits will require some form of common identification.

§ 312.4 Requirements for identification.

Only upon proper identification will any individual be granted access to records which pertain to him/her. Identification is required both for accurate record identification and to avoid disclosing records to unauthorized individuals. Requesters must provide their full name and as much information as possible about the record being sought in order that a proper search for records can be accomplished. Inclusion of a telephone number for the requester is recommended to expedite certain matters. Requesters applying in person must provide an identification with photograph, such as a driver's license, military identification card, building pass, etc.

[59 FR 2746, Jan. 19, 1994]

§ 312.5 Access by subject individuals.

(a) No individual will be allowed access to any information compiled or maintained in reasonable anticipation of civil or criminal actions or proceedings or otherwise exempt under § 312.12. Requests for pending investigations will be denied and the requester instructed to forward another request giving adequate time for the investigation to be completed. Requesters shall be provided the telephone number so they can call and check on the status in order to know when to resubmit the request.

(b) Any individual may authorize the OIG to provide a copy of his/her records to a third part. This authorization must be in writing, must designate the recipient by name, must specify the records or portion to be provided to the recipient, and should accompany the initial request to the OIG.

[56 FR 51976, Oct. 17, 1991, as amended at 59 FR 2746, Jan. 19, 1994]

§ 312.6 Fees.

Requesters will be charged only for the reproduction of requested documents and special postal methods, such